This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-212461**
(43)Date of publication of application : **06.08.1999**

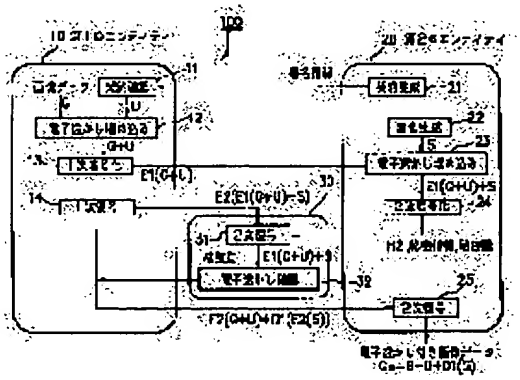
(51)Int.Cl. G09C 5/00
G09C 1/00
H04L 9/32
H04N 1/387
H04N 7/08
H04N 7/081

(21)Application number : **10-013954**
(22)Date of filing : **27.01.1998**

(71)Applicant : **CANON INC**
(72)Inventor : **IWAMURA KEIICHI**

(54) ELECTRONIC WATERMARK SYSTEM AND ELECTRONIC INFORMATION DELIVERY SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic watermark system which surely prevents unauthorized copy of digital data related to copyright.
SOLUTION: The encryption processing and the electronic watermark burying processing of data are distributedly performed in first and second entities (including an author, a selling agent, and a user of data) 10 and 11, and the validity of these encryption processing and electronic watermark burying processing is verified in an independent entity (verification station) 30, thereby surely recognizing the wrong action at the time when the author, the selling agent, or the user wrongfully copies and delivers data. Since check is performed in the verification station in the stage of data delivery from the author to the selling agent and in the stage of that from the selling agent to the user, they cannot do wrong in league with each other, and a system safe against unauthorized delivery of data is realized.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

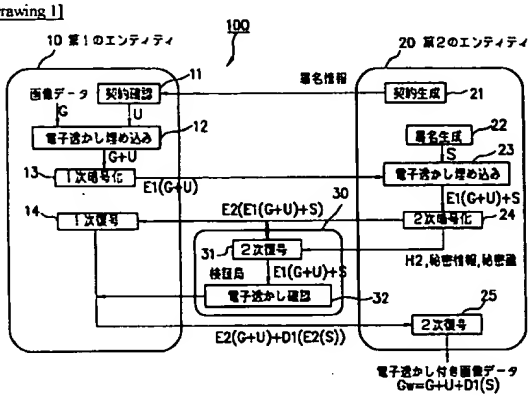
* NOTICES *

Japan Patent Office is not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]



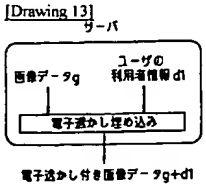
[Drawing 6]

画像ヘッダ部	画像フォーマット識別子
	ファイルサイズ
	X方向ピクセル数（幅）
	Y方向ピクセル数（高さ）
	奥行き方向サイズ
	圧縮の有無
	階層度
	ビットマップへのオフセット
	カラーパレットサイズ
画像データ部	ビットマップ

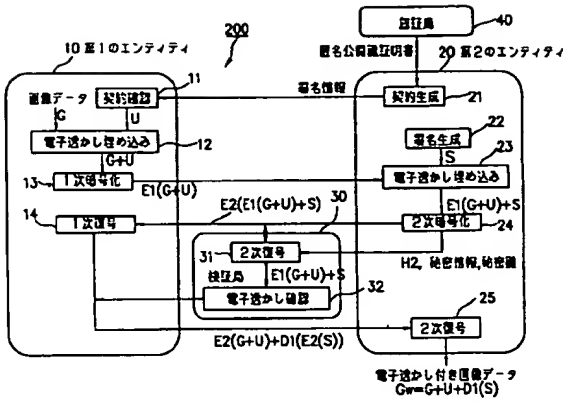
[Drawing 12]

フィールド名	長さ	バイト
画像の幅	4	4-7
画像の高さ	4	8-11
タイルの総数	4	12-15
タイルの幅	4	16-19
タイルの高さ	4	20-23

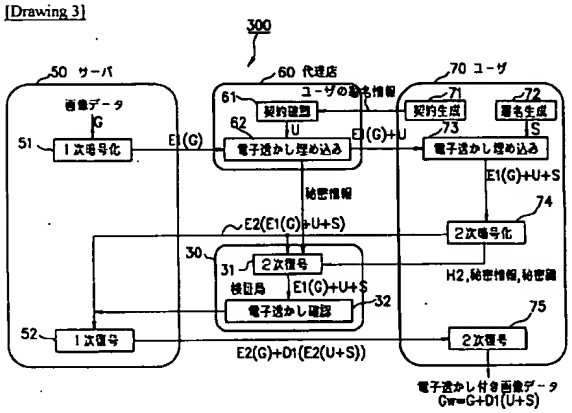
[Drawing 13]



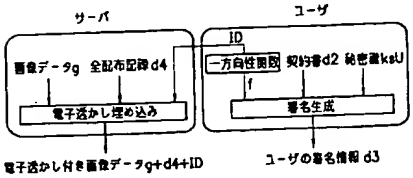
[Drawing 2]



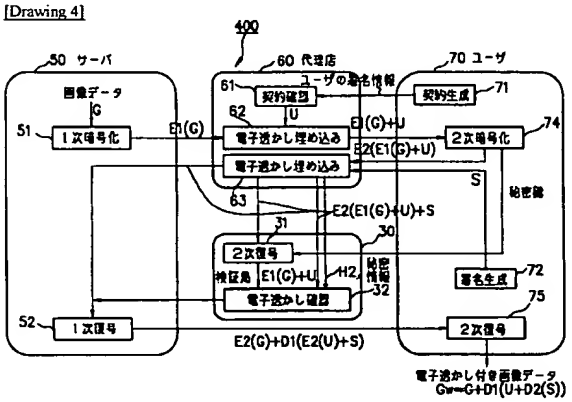
[Drawing 3]



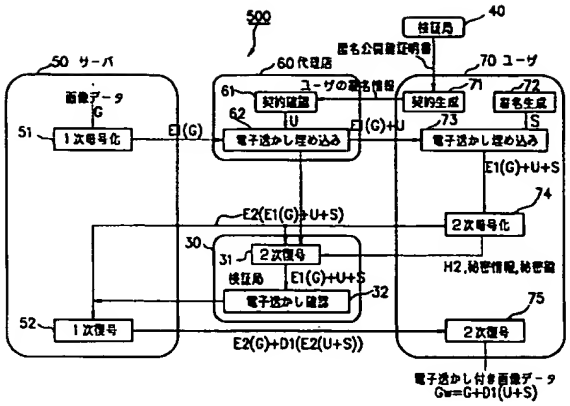
[Drawing 14]



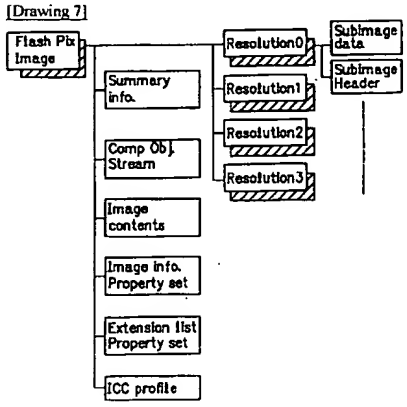
[Drawing 4]



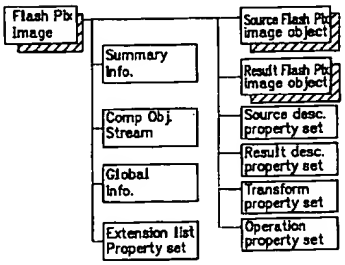
[Drawing 5]



[Drawing 7]



[Drawing 8]



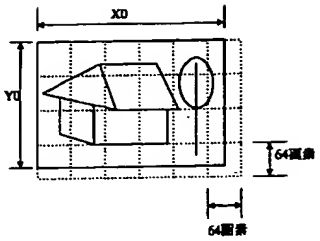
[Drawing 9]

プロパティ名	IDコード	タイプ
画像データの階層数	0x01000000	VT_UI4
最大解像度の画像の幅	0x01000002	VT_UI4
最大解像度の画像の高さ	0x01000003	VT_UI4
初期表示の高さ	0x01000004	VT_R4
初期表示の幅	0x01000005	VT_R4

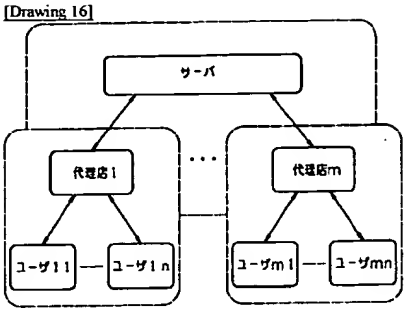
プロパティ名	IDコード	タイプ
ii解像度の画像の幅	0x02ii0000	VT_UI4
ii解像度の画像の高さ	0x02ii0001	VT_UI4
ii解像度の画像の色	0x02ii0002	VT_BLOB
ii解像度の画像を数値で表わしたフォーマット	0x02ii0003	VT_UI4|VT_VECTOR

プロパティ名	IDコード	タイプ
JPEGテーブル	0x03ii0001	VT_BLOB
最大JPEGテーブルのインデックス	0x03000002	VT_UI4

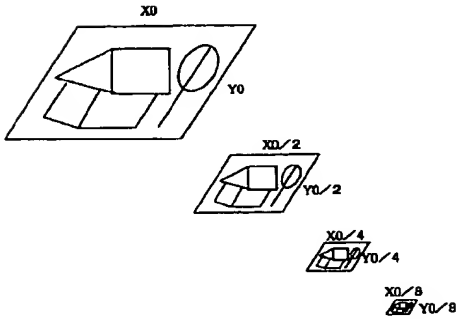
[Drawing 11]



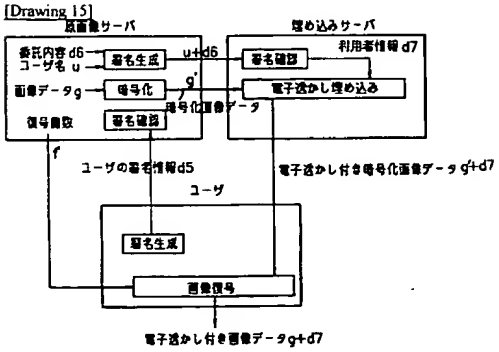
[Drawing 16]



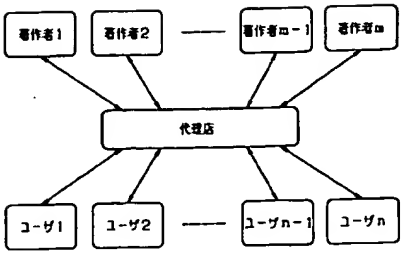
[Drawing 10]



[Drawing 15]



[Drawing 17]



[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing for explaining the digital-watermarking system in which the 1st operation gestalt of this invention was shown.
[Drawing 2] It is drawing for explaining the digital-watermarking system in which the 2nd operation gestalt of this invention was shown.
[Drawing 3] It is drawing for explaining the digital-watermarking system in which the 3rd operation gestalt of this invention was shown.
[Drawing 4] It is drawing for explaining the digital-watermarking system in which the 4th operation gestalt of this invention was shown.
[Drawing 5] It is drawing for explaining the digital-watermarking system in which the 5th operation gestalt of this invention was shown.
[Drawing 6] It is drawing showing a general picture format.
[Drawing 7] It is drawing showing the example of a FlashPixTM file format.
[Drawing 8] It is drawing showing the example of a FlashPixTM file format.
[Drawing 9] It is drawing showing the attribute information stored in Image Content Property Set of a FlashPixTM file format.
[Drawing 10] It is drawing showing the example of the image file which consists of two or more pictures from which resolution differs, respectively.
[Drawing 11] It is drawing showing the situation of tile division of the picture of the layer of each resolution.
[Drawing 12] It is drawing showing the attribute information about the image data by which tile division was carried out.
[Drawing 13] It is drawing for explaining the conventional digital-watermarking system.
[Drawing 14] It is drawing for explaining the conventional digital-watermarking system which improved the method shown in drawing 13 .
[Drawing 15] It is drawing for explaining the conventional digital-watermarking system which improved the method shown in drawing 14 .
[Drawing 16] It is drawing showing an example of the data distribution system constituted hierarchical.
[Drawing 17] It is drawing showing other examples of the data distribution system constituted hierarchical.
[Description of Notations]
10 Terminal Unit by the side of 1st Entity
11 Contract Check Processing Section
12 Digital-Watermarking Embedding Processing Section
13 Primary Encryption Processing Section
14 Primary Decode Processing Section
20 Terminal Unit by the side of 2nd Entity
21 Contract Generation Processing Section
22 Signature Generation Processing Section
23 Digital-Watermarking Embedding Processing Section
24 Secondary Encryption Processing Section
25 Secondary Decode Processing Section
30 Verification Office Terminal Unit
31 Secondary Decode Processing Section
32 Digital-Watermarking Check Processing Section
40 Certificate Authority Terminal Unit
50 Server Terminal Unit
51 Primary Encryption Processing Section
52 Primary Decode Processing Section
60 Agency Terminal Unit
61 Contract Generation Processing Section
62 Digital-Watermarking Embedding Processing Section

63 Digital-Watermarking Embedding Processing Section
70 User-Terminal Equipment
71 Contract Generation Processing Section
72 Signature Generation Processing Section
73 Digital-Watermarking Embedding Processing Section
74 Secondary Encryption Processing Section
75 Secondary Decode Processing Section
100 Electronic-Intelligence Distribution System
200 Electronic-Intelligence Distribution System
300 Electronic-Intelligence Distribution System
400 Electronic-Intelligence Distribution System
500 Electronic-Intelligence Distribution System

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] Especially this invention is used for the digital-watermarking technology for protecting the copyright in digital information, such as dynamic-image data, static-image data, voice data, computer data, and a computer program, and the multimedia network which distributes digital information using it about a digital-watermarking method and an electronic-intelligence distribution system, and is suitable.
[0002]
[Description of the Prior Art] The electronic commerce which deals in goods on a network prospers by development of a computer network in recent years, and the spread of cheap and highly efficient computers. Then, digital data including a picture etc. can be considered as goods dealt with. However, digital data has the property in which a perfect copy can be created easily and in large quantities, this creates unjustly a copy with the user homogeneous as original who bought the digital data, and possibility of saying that a redistribution can be carried out is shown. Thereby originally the price which should be paid to those (henceforth a "vender") to whom sale was commissioned justly is not paid from the author or author of digital data, but it is thought that it infringes on copyright.
[0003] On the other hand, once an author or a vender (those who distribute these digital data justly are summarized hereafter, and it is called a "server") sends digital data to a user, an above-mentioned illegal copy cannot be prevented completely. Therefore, an illegal copy is not prevented directly but the technique called digital watermarking is proposed. By adding operation in original digital data and embedding the copyright information about digital data, and the user information about a user into digital data, this digital watermarking is the technique of specifying who did the redistribution of the data, when an illegal copy is found.
[0004] In the system using the conventional digital watermarking, it is the requisite that a server is the engine which can trust it completely. Therefore, supposing it may perform not an engine but the injustice where a server is reliable, a crime may be forced on the user who is not copying illegally in the conventional system.
[0005] The user by whom this is specified from the user information d1 when a server embeds the user information d1 freely since the server embedded the user information d1 for specifying a user in the conventional system as shown in drawing 13 at the digital data (digital data is hereafter explained as image data) g, and the copy is distributed unjustly is because there is no means to turn down the opinion of a server.
[0006] as the cure -- for example, "-- B. -- Pfitmann and M.Waidner : The system (drawing 14) which used the public key cryptosystem for "Asymmetic Fingerprinting and the reference (it is hereafter described as reference [1]) of "EUROCRYPT'96" is proposed. Here, a cryptographic key and a decode key are the cipher systems which hold public presentation and a decode key for a cryptographic key secretly unlike a public key cryptosystem. The RSA code, ElGamal code, etc. are known as the example of representation. Hereafter, protocols in a public key cryptosystem, such as the (a) feature, (b) secret communication, and authentication communication, are described.
[0007] (a) Since the feature (1) cryptographic key and decode key of public key encryption differ from each other and a cryptographic key can be exhibited, it is not necessary to deliver a cryptographic key secretly, and key delivery is easy.
(2) Since each user's cryptographic key is exhibited, the user should memorize only each one of decode keys in secret.
(3) The authentication function for an addressee checking that the transmitting person of the sent correspondence is not a charlatan and that the correspondence is not altered is realizable.
[0008] (b) If encryption operation performed using the open cryptographic key kp is set to E (kp, M) to Protocol M, for example, the correspondence, of public key encryption and decode operation performed using the secret decode key ks is set to D (ks, M), a public-key-encryption algorithm will fulfill the following two conditions first.
(1) When a cryptographic key kp is given, calculation of the encryption operation E (kp, M) is easy. Moreover, when the decode key ks is given, calculation of the decode operation D (ks, M) is easy.
(2) Even if the user knows the oak and cryptographic key kp which do not know the decode key ks, the computational procedure of the encryption operation E (kp, M), and cipher C=E (kp, M), it is difficult to determine Correspondence M in respect of computational complexity.
[0009] Next, in addition to the conditions of the above (1) and (2), when the following conditions of (3) are satisfied, a secret-communication function is realizable.
(3) The encryption operation E (kp, M) can be defined to all the correspondence (plaintext) M, and D(ks, E (kp, M)) =M is

materialized. That is, since the cryptographic key kp is exhibited, although everyone can calculate encryption operation E (kp, M), D (ks, E (kp, M)) can be calculated and only he with the secret decode key ks can get Correspondence M.
[0010] On the other hand, in addition to the conditions of the above (1) and (2), when the following conditions of (4) are satisfied, authentication communication facility is realizable.
(4) The decode operation D (ks, M) can be defined to all the correspondence (plaintext) M, and E(kp, D (ks, M)) =M is materialized. That is, it is only he with the secret decode key ks that calculation of the decode operation D (ks, M) can be performed. Though other men turn into him who calculates D (ks', M) using fake secret decode key ks', and has the secret decode key ks and finish, it is E (since it is kp and D(ks', M) !=M, it can check that the received information of an addressee is unjust.). Moreover, even if the value of D (ks, M) is altered, it is set to E(kp, D(ks, M)') !=M, and can check that the received information of an addressee is unjust.
[0011] In the above public key cryptosystems, processing [using "encryption" and the secret decode key (henceforth a private key) ks]-processing E() which uses open cryptographic key (henceforth public key) kp D() is called "decode." Therefore, although a transmitting person enciphers and an addressee performs decode after that in secret communication, in authentication communication, a transmitting person will perform decode and an addressee will encipher after that.
[0012] A protocol in case a public key cryptosystem performs secret communication, authentication communication, and secret communication with a signature to below from the transmitting person A to Addressee B is shown. Here, the transmitting person's A private key is set to ksA, a public key is set to kpA, the private key of Addressee B is set to ksB, and a public key is set to kpB.
[0013] When carrying out secret communication of the correspondence (plaintext) M from [secret-communication] transmitting person A to Addressee B, the following procedure performs.
Step1: The transmitting person A enciphers Correspondence M as follows with the public key kpB of Addressee B, and sends Cipher C to Addressee B.
C=E(kpB,M)
Step2: Addressee B decodes Cipher C as follows with its own private key ksB, and obtains the plaintext M of a basis.
M=D(ksB,C)
In addition, since the public key kpB of Addressee B is opened to many and unspecified persons, the secret communication not only of the transmitting person A but all the men can be carried out to Addressee B.
[0014] When carrying out authentication communication of the correspondence (plaintext) M from the [authentication communication] transmitting person A to Addressee B, the following procedure performs.
Step1: The transmitting person A generates the transmitting sentence S as follows with his own private key ksA, and sends to Addressee B.
S=D(ksA,M)
This transmitting sentence S is called "signature sentence", and operation of obtaining the signature sentence S is called "signature."
Step2: Addressee B carries out restoration conversion of the signature sentence S as follows with the transmitting person's A public key kpA, and obtains the plaintext M of a basis.
M=E(kpA,S)
Supposing Correspondence M checks that it is a meaningful sentence, it will attest that surely Correspondence M has been sent by the transmitting person A. Since the transmitting person's A public key kpA is opened to many and unspecified persons, not only the addressee B but all men can attest the transmitting person's A signature sentence S. Such authentication is called "digital signature."
[0015] When carrying out secret communication with a signature of the correspondence (plaintext) M from the [secret communication with signature] transmitting person A to Addressee B, the following procedure performs.
Step1: The transmitting person A signs Correspondence M as follows with his own private key ksA, and makes the signature sentence S.
S=D(ksA,M)
Furthermore, the transmitting person A enciphers the signature sentence S as follows with the public key kpB of Addressee B, and sends Cipher C to Addressee B.
C=E(kpB,S)
Step2: Addressee B decodes Cipher C as follows with its own private key ksB, and obtains the signature sentence S.
S=D(ksB,C)
Furthermore, Addressee B carries out restoration conversion of the signature sentence S as follows with the transmitting person's A public key kpA, and obtains the plaintext M of a basis.
M=E(kpA,S)
Supposing Correspondence M checks that it is a meaningful sentence, it will attest that surely Correspondence M has been sent by the transmitting person A.
[0016] In addition, you may reverse the sequence of giving the function in each Step of secret communication with a signature, respectively. That is, by the above-mentioned procedure, it is Step1:C=E (kpB, D (ksA, M)).
Step2:M=E(kpA,D(ksB,C))
Although it has become, secret communication with a signature is realizable with the following procedures.
Step1:C=D(ksA,E(kpB,M))

Step2:M=D(ksB,E(kpA,C))
[0017] The procedure of the operation in the system (above-mentioned drawing 14) using the conventional digital watermarking which applied the above public key cryptosystems to below is shown.
1) Exchange the contract d2 about dealing of image data g between a server and a user first.
[0018] 2) Next, a user generates the random number ID in which he is shown, and, on the other hand, generates the tropism function f using this. On the other hand, the thing with this easy thing [asking for y from x] for which x is but calculated from y conversely says a difficult function as a tropism function in function y=f (x). for example, the factorization in prime numbers to the big integer of a number of digits -- dispersed -- on the other hand, a logarithm etc. is well used as a tropism function
3) Next, a user generates [as opposed to / the tropism function f / on the other hand] the signature information d3 using his own private key ksU with a contract d2, doubles them, and sends to a server.
[0019] 4) Next, a server checks the signature information d3 and a contract d2 using a user's public key kpU.
5) A server embeds after a check all distribution records d4 by present, and the random number ID which the user created at image data g, and generates image data with digital watermarking (g+d4+ID).
6) A server sends the image data with digital watermarking (g+d4+ID) to a user.
[0020] Then, when an illegal copy is discovered, it embeds from the inaccurate image data, information is extracted, and a user is specified from ID contained there. At this time, the thing of the following [be / what was distributed without notice by the server / the illegal copy] is asserted as a basis. Since a signature of a user is attached to the tropism function value f while it was generated by the user itself and it was used, I hear that ID as which it specifies a user cannot generate such ID to arbitrary users, and it has a server. However, in order that the user who contracted formally between servers may send ID which specifies itself to a server, forcing of the crime of YUZAHE is possible for forcing of the crime to the user who contracted formally too, and a contract of is not made only becomes impossible.
[0021] Then, the system (drawing 15) by which forcing of a crime becomes impossible is proposed by the user who contracted formally at the reference (it is hereafter described as reference [2]) of "Miura, Watanabe, **(Nara nose-of-cam size): "digital watermarking also in consideration of the injustice of a server", SCIS97-31C." This is realized by embedding a server with a subject-copy image server, and dividing into a server. However, in this system, digital watermarking embedded at the time of encryption and decode is carried out, if not destroyed. Hereafter, the procedure of the operation in the system of above-mentioned drawing 15 is shown.
[0022] 1) First, a user attaches signature d5 and demands desired image data of a subject-copy image server.
2) A subject-copy image server checks the content of a demand from the signature d5 of a user, enciphers and embeds image data g demanded after the check, and sends it to a server. At this time, a subject-copy image server attaches and embeds the signature to user name u and the content d6 of consignment, and sends it to a server. It can come, simultaneously a subject-copy image server sends decode function f' to encryption to a user.
[0023] 3) An embedding server checks sent encryption image data g' and a signature (u+d6), performs the creation and embedding of the user information d7 which specify a user based on user name u and the content d6 of consignment, and creates encryption image data with digital watermarking (g'+d7). Then, an embedding server sends the encryption image data with digital watermarking (g'+d7) to a user.
4) A user decodes encryption image data with digital watermarking (g'+d7) with image data (g+d7) HE with digital watermarking using decode function f' sent from the subject-copy image server.
[0024] Then, when an illegal copy is discovered, a subject-copy image server enciphers and embeds the inaccurate image data, extracts information, embeds it, and sends it to a server. An embedding server specifies a user from this embedding information. in this system, a subject-copy image server does not embed the user information d7 for specifying a user at image data g, and an embedding server does not know decode function f' (return a picture -- there is nothing) -- it is -- it is making into the basis for each server to be unable to carry out unjust distribution of the image data which embedded a user's user information d7 without notice to the user who contracted formally
[0025] However, by the system of this drawing 15 , it embeds with a subject-copy image server, and does not take into consideration about conspiracy with a server, and conspiracy with an embedding server and a user is not considered, either. Therefore, the injustice of a server is possible like [since it has encryption image data g' of image data g whose embedding server is a subject-copy image and a user has decode function f', when it embeds with a subject-copy image server and a server conspires] the system of above-mentioned drawing 14 , and when an embedding server and a user conspire, unjust acquisition of a subject-copy image is possible.
[0026] Moreover, if management of a user's decode function f' is inadequate, even if an embedding server does not conspire with a user, possibility that decode function f' can be known from a user's inattention etc. is large, although a subject-copy image server sends decode function f' to a user.
[0027] Furthermore, although the subject-copy image server is carried out in this system if it does not have an embedding means or the right embedding cannot do it, since a subject-copy image server extracts embedding information, if embedding information is analyzed, it will be thought that possibility that a subject-copy image server can perform the right embedding now is high. And the same injustice as the system of above-mentioned drawing 14 is possible in this case.
[0028] Furthermore, as mentioned above, although the system which consists of a user and a server was conventionally proposed with imperfection, the safe system in case the element related to dealing of image data is constituted hierarchical was not proposed. To be shown in drawing 16 as an example of a hierarchical system, it is the system that two or more

agencies are under a server, and a user is in the bottom of it, or sale of the image data which requires two or more authors for its writing is requested from a certain sales agent to be shown in drawing 17 , and it thinks of the agency which received the request as a system of selling two or more authors' image data to many users.
[0029] In these hierarchical systems, in order that the elements which constitute dealing of image data may increase in number from an above-mentioned server and two persons of a user to three persons of a server (or author), an agency, and a user, as for the problem of conspiracy etc., a component becomes more complicated than two persons' system. That is, the system of above-mentioned drawing 15 is reference [2], although it will be thought that a server, an agency, and a user are the systems of a component, if it thinks widely. It is not a thing supposing the hierarchical system, a server is divided from a viewpoint of preventing the injustice of one server, and the problem of conspiracy is not taken into consideration as mentioned above, either.
[0030]
[Problem(s) to be Solved by the Invention] this invention is accomplished in view of such the actual condition, and it aims at offering the digital-watermarking method and electronic-intelligence distribution system which can prevent the above injustice certainly. Especially this invention aims at the element related to dealing of a work enabling it to prevent the injustice by conspiracy certainly in the system constituted hierarchical.
[0031]
[Means for Solving the Problem] The digital-watermarking method of this invention is characterized by verifying one [at least] justification of the above-mentioned cipher processing which distributed by two or more meanses or entities, performed cipher processing and digital-watermarking embedding processing to data, and was performed by the means or entity of the above-mentioned plurality, and digital-watermarking embedding processing by the means, the means different from an entity, or entity of the above-mentioned plurality. Here, the meanses or entities of the above-mentioned plurality may be at least three or more sorts of meanses or entities.
[0032] For example, the means or entity of the above-mentioned plurality may consist of the 1st entity which has a means to perform the 1st cipher processing to data, the 2nd entity which has a means to perform the above-mentioned digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above, and the 3rd entity which has a means to perform the 2nd cipher processing and uses data with digital watermarking.
[0033] Moreover, the means or the entity of the above-mentioned plurality has the 1st entity which has a means perform the 1st cipher processing to data, the 2nd entity which has a means perform the above-mentioned digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above, and a means perform a means perform the above-mentioned digital-watermarking embedding processing, and 2nd cipher processing, and may consist of the 3rd entity using data with digital watermarking.
[0034] Moreover, the means or the entity of the above-mentioned plurality may consist of the 1st entity which has a means perform a means perform the above-mentioned digital-watermarking embedding processing to data, and 1st cipher processing, the 2nd entity which has a means perform the above-mentioned digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above, and the 3rd entity which has a means perform the 2nd cipher processing and uses data with digital watermarking.
[0035] Furthermore, the means or entity of the above-mentioned plurality The 1st entity which has a means to perform a means to perform the above-mentioned digital-watermarking embedding processing to data, and 1st cipher processing, The 2nd entity which has at least one of the meanses which performs a means to perform the above-mentioned digital-watermarking embedding processing, a means to perform the 1st cipher processing, and 2nd cipher processing, and manages and distributes the data from the 1st entity of the above, It has a means to perform a means to perform the above-mentioned digital-watermarking embedding processing, and 2nd cipher processing, and you may consist of the 3rd entity using data with digital watermarking.
[0036] In the above-mentioned composition, the above-mentioned entity may be made to encipher to the data with which digital watermarking was embedded. Moreover, you may make it the above-mentioned entity embed digital watermarking to the data with which encryption was given.
[0037] Moreover, you may make it the 2nd entity of the above embed digital watermarking to the data with which the 1st cipher processing of the above from the 1st entity of the above was performed. Moreover, you may make it the 2nd entity of the above embed digital watermarking to the data with which the 2nd cipher processing of the above from the data with which the 1st cipher processing of the above from the 1st entity of the above was performed, and the 3rd entity of the above was performed. Moreover, you may make it the 2nd entity of the above output the value which, on the other hand, changed the data with which the 2nd cipher processing of the above was performed with the tropism function. Moreover, you may make it the 2nd entity of the above transmit the value changed with the above-mentioned 1 directivity function to the 4th entity of the above.
[0038] Moreover, you may make it output the 3rd entity of the above with the data with which the value which, on the other hand, changed the data with which the 2nd cipher processing of the above was performed with the tropism function was given to the 2nd cipher processing of the above. Moreover, you may make it the 3rd entity of the above transmit the value changed with the above-mentioned 1 directivity function to the 4th entity of the above. Moreover, the 3rd entity of the above receives the information enciphered primarily beforehand, and may be made to give secondary encryption to the this enciphered information.
[0039] Moreover, the 4th entity of the above can perform decode processing corresponding to the 2nd cipher processing of

the above, and is good to also make. Moreover, you may make it the 4th entity of the above have a means to manage a cryptographic key. Moreover, you may make it the 4th entity of the above verify one [at least] justification of the above-mentioned digital watermarking and cipher processing by decrypting the data which are outputted from other entities and with which it was enciphered and digital watermarking was embedded. Moreover, you may make it the 4th entity of the above verify one [at least] justification of the above-mentioned digital watermarking and cipher processing by comparing the value which, on the other hand, changed the data which are outputted from an entity besides the above, and with which it was enciphered and digital watermarking was embedded with the tropism function with the value outputted from an entity besides the above.

[0040] Moreover, the electronic-intelligence distribution system of this invention is set to the electronic-intelligence distribution system which transmits and receives digital data on the network system which consists of two or more entities. The 1st entity which has a means to perform the 1st cipher processing to data, The 2nd entity which has a means to perform digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above, It is characterized by having a means to perform the 2nd cipher processing and having the 4th entity which verifies one [at least] justification of cipher processing performed by the 3rd entity using data with digital watermarking, and the above 1st - the 3rd entity, and digital-watermarking embedding processing.

[0041] In the electronic-intelligence distribution system which transmits and receives digital data in other modes of this invention on the network system which consists of two or more entities The 1st entity which has a means to perform the 1st cipher processing to data, The 2nd entity which has a means to perform digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above, The 3rd entity which has a means to perform a means to perform the above-mentioned digital-watermarking embedding processing, and 2nd cipher processing, and uses data with digital watermarking, It is characterized by having the 4th entity which verifies one [at least] justification of cipher processing performed by the above 1st - the 3rd entity, and digital-watermarking embedding processing.

[0042] In the electronic-intelligence distribution system which transmits and receives digital data in the mode of others of this invention on the network system which consists of two or more entities The 1st entity which has a means to perform a means to perform digital-watermarking embedding processing to data, and 1st cipher processing, The 2nd entity which has a means to perform the above-mentioned digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above, It is characterized by having a means to perform the 2nd cipher processing and having the 4th entity which verifies one [at least] justification of cipher processing performed by the 3rd entity using data with digital watermarking, and the above 1st - the 3rd entity, and digital-watermarking embedding processing.

[0043] In the electronic-intelligence distribution system which transmits and receives digital data in the mode of others of this invention on the network system which consists of two or more entities The 1st entity which has a means to perform a means to perform digital-watermarking embedding processing to data, and 1st cipher processing, The 2nd entity which has at least one of the meanses which performs a means to perform the above-mentioned digital-watermarking embedding processing, a means to perform the 1st cipher processing, and 2nd cipher processing, and manages and distributes the data from the 1st entity of the above, The 3rd entity which has a means to perform a means to perform the above-mentioned digital-watermarking embedding processing, and 2nd cipher processing, and uses data with digital watermarking, It is characterized by having the 4th entity which verifies one [at least] justification of cipher processing performed by the above 1st - the 3rd entity, and digital-watermarking embedding processing.

[0044] Here, the 4th entity which performs the above-mentioned verification may be an entity which manages a cryptographic key. Moreover, the digital-watermarking information which the 1st entity of the above embeds may also include the information about the 3rd entity of the above. Moreover, the digital-watermarking information which the 1st entity of the above embeds may also include the information about the digital data which transmits. Moreover, the digital-watermarking information which the 2nd entity of the above embeds may also include the information about the 3rd entity of the above. Moreover, the digital-watermarking information which the 3rd entity of the above embeds may be information which can create only the 3rd entity of the above. Moreover, the 1st entity of the above may be made to perform the above-mentioned digital-watermarking embedding processing, after verifying the signature of the 3rd entity of the above with the anonymity public key with a certificate published by the certificate authority. Moreover, the 2nd entity of the above may be made to perform the above-mentioned digital-watermarking embedding processing, after verifying the signature of the 3rd entity of the above with the anonymity public key with a certificate published by the certificate authority.

[0045]

[Embodiments of the Invention] [1st operation gestalt] The 1st operation gestalt concerning this invention is hereafter explained with reference to drawing 1 . The digital-watermarking method concerning this invention is carried out by the system 100 as shown in drawing 1 , and this system 100 is also what applied the electronic-intelligence distribution system concerning this invention.

[0046] That is, a system 100 is a network system which consists of an entity (not shown) of a large number containing the terminal unit 10 by the side of the 1st entity (it is hereafter described as the 1st terminal unit), the terminal unit 20 by the side of the 2nd entity (it is hereafter described as the 2nd terminal unit), and the terminal unit 30 by the side of a verification office (it is hereafter described as a verification office terminal unit), and each entity is made as [receive / deliver and / digital data / mutually / through a network].

[0047] The contract check processing section 11 to which, as for the 1st terminal unit 10, the data from the 2nd terminal unit 20 are supplied, For example, the digital-watermarking embedding processing section 12 to which the output of image data

(digital data) and the contract check processing section 11 is supplied, The primary encryption processing section 13 to which the output of the digital-watermarking embedding processing section 12 is supplied, It has the primary decode processing section 14 to which the data from the 2nd terminal unit 20 are supplied, and is made as [transmit / each output of the primary encryption processing section 13 and the primary decode processing section 14 / to the 2nd terminal unit 20].

[0048] Moreover, the contract generation processing section 21 to which the 2nd terminal unit 20 transmits data to the contract check processing section 11 of the 1st terminal unit 10, The signature generation processing section 22 and the digital-watermarking embedding processing section 23 to which the data from the signature generation processing section 22 and the primary encryption processing section 13 of the 1st terminal unit 10 are supplied, The secondary encryption processing section 24 to which the output of the digital-watermarking embedding processing section 23 is supplied, It has the secondary decode processing section 25 to which the data from the primary decode processing section 14 of the 1st terminal unit 10 are supplied, and is made as [output / as image data with digital watermarking / the output of the secondary decode processing section 25]. Moreover, the output of the secondary encryption processing section 24 is made as [supply / respectively / the primary decode processing section 14 of the 1st terminal unit 10 and the verification office terminal unit 30].

[0049] Moreover, the verification office terminal unit 30 is equipped with the secondary decode processing section 31 to which the data from the secondary encryption processing section 24 of the 2nd terminal unit 20 are supplied, and the digital-watermarking check processing section 32 to which the output of the secondary decode processing section 31 is supplied, and is made as [supply / the output of the digital-watermarking check processing section 32 / to the 1st terminal unit 10 and the 2nd terminal unit 20]. Moreover, the output of the secondary decode processing section 31 is made as [supply / the primary decode processing section 14 of the 1st terminal unit 10].

[0050] In the electronic-intelligence distribution system of this operation gestalt constituted as mentioned above, below, it divides into the 1st embedded processing at the time of the server or author who showed drawing 16 or drawing 17 handing an agency digital data, and the 2nd embedded processing at the time of an agency handing a user digital data, and thinks. This operation gestalt is realized using the same protocol which shows the 1st embedded processing and the 2nd embedded processing below. The whole processing performs 2nd embedded processing, after performing 1st embedded processing.

[0051] In the following explanation, by 1st embedded processing, the 1st above-mentioned entity means a server or an author, and the 2nd entity means an agency by it. Moreover, by 2nd embedded processing, the 1st entity means an agency, and the 2nd entity means a user by it. Therefore, the terminal unit used in an agency at least has each processing sections of all with which the 1st terminal unit 10 and the 2nd terminal unit 20 of drawing 1 were equipped.

[0052] The concrete protocol which realizes embedded processing of the above 1st and 2nd embedded processing is explained below, referring to drawing 1 . In this protocol, the information about primary codes, such as a method and a private key, is information which only the 1st entity knows, and the information about a secondary code is information which only the 2nd entity knows. However, among these codes, it shall have the property in which the code will be solved if decode is performed whichever it performs encryption previously. Encryption shall be hereafter expressed with "Ei()", decode shall be expressed with "Di()", and the embedding processing about digital watermarking shall be expressed with "+."

[0053] Below, operation of the system 100 constituted as mentioned above is explained. First, the embedding processing about digital watermarking is explained.

[0054] [embedding processing] 1 -- first, in the 2nd terminal unit 20, the 2nd entity attaches a signature and desired image data is required of the 1st terminal unit 10 (the 1st entity) This demand data is the signature information generated by the contract generation processing section 21, and, below, calls this contract information.

[0055] 2) Next, in the 1st terminal unit 10, the 1st entity checks the contract information received using the contract check processing section 11 from the signature of the 2nd entity, and creates the user information U from contract information after the check. And the digital-watermarking embedding processing section 12 is embedded at image data G of which the user information U created in the above-mentioned contract check processing section 11 was required. Moreover, the primary encryption processing section 13 performs primary encryption processing E1 () to the image data (G+U) where the user information U was embedded in the digital-watermarking embedded processing section 12, and sends the obtained data to the 2nd terminal unit 20. Therefore, the information on the primary encryption image data E1 (G+U) will be sent to the 2nd terminal unit 20.

[0056] 3) Next, in the 2nd terminal unit 20, the signature generation processing section 22 generates the signature information S using the private key of the 2nd entity. And the digital-watermarking embedding processing section 23 embeds the signature information S generated in the signature generation processing section 22 at the primary (distributed) encryption image data E1 (G+U) sent from the 1st terminal unit 10. Moreover, the secondary encryption processing section 24 enciphers secondary primary encryption image data E1(G+U)+S where the signature information S was embedded in the digital-watermarking embedding processing section 23, and sends it to the verification office terminal unit 30. Therefore, the information on the secondary encryption image data E2 (E1(G+U) +S) will be sent to the verification office terminal unit 30.

[0057] At this time, the secondary encryption processing section 24 generates and signs the hash value H2 to the transmit data (secondary encryption image data E2 (E1(G+U) +S)) to the verification office terminal unit 30, and sends both the confidential information relevant to digital watermarking except the signature information S, and the private key of secondary encryption to the verification office terminal unit 30. In addition, confidential information is information about the embedding position and intensity for detecting digital watermarking, and it is enciphered and sent by other cipher systems currently shared with the verification office terminal unit 30.

[0058] Moreover, generally a hash value is an output value of Hash Function h(), and a Hash Function means the compressibility function which cannot cause a collision easily. Here, a collision is with h(x1) =h (x2) and a bird clapper to a different value x1 and different x2. Moreover, a compressibility function is a function which changes the bit string of arbitrary bit length into the bit string of a certain length. Therefore, a Hash Function is function h() which changes the bit string of arbitrary bit length into the bit string of a certain length, and the value x1 and x2 which fill h(x1) =h (x2) cannot be found out easily. Since the value x with which any value y to y=h (x) is filled cannot be easily found out at this time, on the other hand, a Hash Function turns into a tropism function inevitably. As an example of this Hash Function, MD (Message Digest)5, SHA (Secure Hash Algorithm), etc. are known.
[0059] 4) Next, in the verification office terminal unit 30, check being [of the hash value H2 sent from the 2nd terminal unit 20] a signature, and that the hash value H2 is in agreement with the hash value of transmit data, and after the check, the secondary decode processing section 31 decodes the secondary encryption image data E2 (E1(G+U) +S) from the 2nd terminal unit 20, and extracts the signature information S from there. And the signature information S is inspected in the digital-watermarking check processing section 32, if right, verification information will be created and the signature of the verification office terminal unit 30 will be attached. Finally, the verification office terminal unit 30 sends the information on the secondary encryption image data E2 (E1(G+U) +S) transmitted from the 2nd terminal unit 20, a hash value H2, its signature and the verification information over it, and its signature to the 1st terminal unit 10.
[0060] 5) Next, in the 1st terminal unit 10, the 1st entity checks the verification information sent from the verification office terminal unit 30, and its signature, and checks the secondary [further] encryption image data E2 (E1(G+U) +S), a hash value H2, and its signature. After the check, the primary decode processing section 14 decodes primary encryption of the above-mentioned secondary encryption image data E2 (E1(G+U) +S), generates the information on E2(G+U)+D1 (E2 (S)), and sends it to the 2nd terminal unit 20.
[0061] 6) Next, in the 2nd terminal unit 20, the secondary decode processing section 25 decodes secondary encryption of the information on E2(G+U)+D1 (E2 (S)) sent from the 1st terminal unit 10, and takes out the image data Gw with digital watermarking. Therefore, the image data Gw with digital watermarking is expressed as Gw=G+U+D1 (S). This shows that the user information U and the signature information S on the 2nd entity influenced of primary decode space to image data G of a basis, and it is embedded as information.
[0062] When the right watermark information is not verified with the verification office terminal unit 30 in the process of the above 4 according to one of the injustice of the 1st entity or the 2nd entity, the 1st terminal unit 10 and the 2nd terminal unit 20 are told about that. Even if dealings are stopped at this time, although the 1st entity cannot acquire a price, unjust acquisition of the image data is not carried out at the 2nd entity, and although the 2nd entity cannot receive image data, it does not pay a price to the 1st entity. Therefore, there is no meaning of the 1st entity and the 2nd entity which profits and disadvantageous profit are meaningless and both carries out injustice.
[0063] That is, if the above-mentioned digital-watermarking embedding processing is performed, in the 1st embedded processing, the agency which is the 2nd entity can get the image data Gw with digital watermarking which embedded its signature information S to the subject-copy image data G of the server which is the 1st entity, or an author. In addition, if the 1st user information and signature information in embedded processing are set to U1 and S1, respectively, the image data Gw with digital watermarking which an agency gets will be set to Gw=G+U1+D1 (S1).
[0064] next, the user who will become the 2nd entity in the 2nd embedded processing about the image data Gw with digital watermarking which the agency got at this time if embedding processing same as a subject-copy image is performed (let an agency be the 1st entity) -- with digital watermarking -- image data Gww=G+U1+D1(S1)+U2+D3 (S2) can be obtained However, the encryption which sets the 2nd user information and signature information in embedded processing to U2 and S2, respectively, and an agency performs shall be expressed with E3(), and decode shall be expressed with D3 ().
[0065] When an illegal copy (unjust picture) is discovered, an inaccurate person can be easily specified by the easy following verification processings. The verification processing described below is also divided into the 1st verification processing which is verification processing between the server or author corresponding to the 1st embedded processing, and an agency, and the 2nd verification processing which is verification processing between the agency corresponding to the 2nd embedded processing, and a user, and is performed. The turn performs 1st verification processing first, and, next, performs 2nd verification processing.
[0066] However, in the 1st verification processing, the following user information and signature information are U1 and S1, and the encryption and the decode which an agency performs are E3() and D3(). Moreover, in the 2nd verification processing, the following user information and signature information are U2 and S2. In addition, here above-mentioned reference [1] [2] Image data sets similarly assumption of not receiving deformation and elimination of watermark information.
[0067] [verification processing] 1 -- the unjust picture Gw which the 1st entity discovered in the 1st terminal unit 10 by the 1st verification processing first -- '=G+U' -- user information U' is extracted from +D1 (S'), the primary above-mentioned unjust picture Gw' is enciphered further, and signature information S' is extracted When user information U' is not extracted here, it presumes that the 1st entity is inaccurate.
[0068] 2) When the right signature information is extracted in the 1st verification processing, progress to the 2nd verification processing (when it is S'=S). When same processing is performed also in the 2nd verification processing and the right signature information is extracted, it presumes that the 2nd entity is inaccurate. Being able to create [but] the signature information that this is right, only to the 2nd entity, the 1st entity is because signature information cannot be known. 3) Moreover, when the right signature information is not extracted, presume that the 1st entity is inaccurate (when it is S'!=S).

[0069] By the digital-watermarking method by this 1st operation gestalt, since encryption processing of digital data and embedding processing of digital-watermarking information are performed with both the 1st terminal unit 10 and the 2nd terminal unit 20 and the verification office terminal unit 30 is checking justification of cipher processing and the embedded digital-watermarking information, even if the 1st entity or the 2nd entity copies illegally independently, the malfeasance can be checked easily, and an inaccurate person can also verify easily.
[0070] Moreover, by this method, since inspection by the verification office is conducted for every processing of the 1st embedded processing and the 2nd embedded processing, conspiracy does not have a meaning but there cannot be no conspiracy [which] with a server or an author, an agency, and a user. Even if it conspires, a malfeasance can be checked easily. In addition, the safety of this processing puts a basis on a verification office being reliable.
[0071] [2nd operation gestalt] The currency on the network called electronic cash is being realized in recent years. Since an owner's name does not describe this electronic cash like the usual cash, anonymity is realized. When anonymity is not realized, the seller of goods can know the information who purchased which goods from electronic cash, and a user's privacy will be committed. For this reason, realization of a user's privacy protection as well as the protection of copyrights of the author by digital watermarking mentioned above is important.
[0072] Then, when a user's anonymity is realized at the time of purchase and injustice like unjust distribution of a picture is discovered, it enables it to specify the unjust distribution person who is the purpose of original of digital watermarking with this 2nd operation gestalt. This is realized by the system 200 as shown in drawing 2 . Although this system 200 is considered as the same composition as the system 100 in the 1st operation gestalt mentioned above, it is considered as the composition with which the anonymity public key certificate from a certificate authority 40 is given to the 2nd terminal unit 20.
[0073] Usually, in order to prove the justification, the certificate by the engine called certificate authority is given to the public key which inspects signature information in many cases. This certificate authority means the engine which publishes a certificate to a user's public key, in order to guarantee the justification of a user's public key in a public key cryptosystem. That is, a certificate authority draws up and publishes a certificate by signing the data about a user's public key or a user with the private key of a certificate authority. Other users to whom its own public key with a certificate was sent from a certain user attest the justification (say at least that it is the user accepted by the certificate authority) of the user who has sent the public key by inspecting this certificate with the public key of a certificate authority. As an organization which is managing such a certificate authority, a company called VeriSign and CyberTrust is known well.
[0074] Therefore, when an agency checks a user's contract information from a signature in the procedure of two under 2nd embedded processing stated with the 1st operation gestalt mentioned above, it is possible to check with a public key with the certificate of the certificate authority 40 of drawing 2 . However, in this certificate, the name of the owner of a public key is usually describing. Therefore, the anonymity of the user at the time of the purchase of data will be realized in this case.
[0075] On the other hand, if a certificate authority 40 holds correspondence with a public key and its owner secretly, an owner's name cannot be described in the certificate of a public key, either. The certificate of the public key which has such anonymity is henceforth called "anonymity public key certificate", and such a public key with a certificate is called "anonymity public key with a certificate." Then, if a user sends the anonymity public key with a certificate for inspecting the signature of contract information, and the signature information S together with contract information in the procedure of one under 2nd embedded processing mentioned above, a user can make himself anonymity at the time of the purchase of digital data.
[0076] Therefore, although an anonymity public key with a certificate is passed to an agency as information which specifies a user, at the time of discovery of an illegal copy, a user can be specified by showing the anonymity public key with a certificate in a certificate authority 40, and having a user corresponding to the public key taught. Both the anonymity at the time of a user's digital data purchase and the inaccurate person specification at the time of unjust discovery are realizable by changing as follows 1 under 2nd embedded processing stated with the 1st operation gestalt mentioned above from the above thing, the procedure of 2, and the procedure of one under 2nd verification processing.
[0077] Hereafter, the embedding processing in the system 200 of above-mentioned drawing 2 and verification processing are explained concretely.
[0078] [embedding processing] 1 -- first, in the 2nd terminal unit 20, together with the anonymity public key with a certificate published by the certificate authority 40, the contract generation processing section 21 attaches the signature corresponding to the public key for the contract information which requires desired image data, and sends it to the 1st terminal unit 10
2) Next, in the 1st terminal unit 10, the contract check processing section 11 checks the signature of contract information from the anonymity public key of the 2nd entity, and creates the user information U from either contract information or an anonymity public key with a certificate at least after the check while it inspects the public key of the 2nd entity with the public key of a certificate authority 40. And after embedding at image data G of which the user information U created by the digital-watermarking embedding processing section 12 in the above-mentioned contract check processing section 11 was required, the primary encryption processing section 13 performs primary encryption processing E1 (), and the obtained data are sent to the 2nd terminal unit 20. Therefore, the information on the primary encryption image data E1 (G+U) is sent to the 2nd terminal unit 20. Since the following procedures of 3-6 are the same as the procedure stated with the 1st operation gestalt, the explanation which overlaps here is omitted.
[0079] [verification processing] 1 -- by the 2nd verification processing, the 1st terminal unit 10 extracts user information from discovered unjust picture Gww', enciphers primary unjust picture Gww' further, and extracts signature information Furthermore, the anonymity public key which the extracted user information and contract information show is shown in a

certificate authority 40, and the 2nd entity name corresponding to the anonymity public key is heard. When user information is not extracted here, it presumes that the 1st entity is inaccurate. The following procedures of 2 and 3 are the same as the procedure stated with the 1st operation gestalt.

[0080] As stated above, according to the 2nd operation gestalt, anonymity can maintain a user also to a verification office at the time of the purchase of digital data.

[0081] [3rd operation gestalt] With the 3rd operation gestalt, the server or author who showed drawing 16 or drawing 17 considers collectively the processing which distributes digital data among a user through an agency. Hereafter, the 3rd operation gestalt concerning this invention is explained, referring to drawing 3 . That is, the digital-watermarking method concerning the 3rd operation gestalt is carried out by the system 300 as shown in drawing 3 , and this system 300 is also what applied the electronic-intelligence distribution system concerning this invention.

[0082] The system 300 concerning the 3rd operation gestalt The terminal unit by the side of a server The terminal unit by the side of 50 and an agency (It is hereafter described as a server terminal unit) The terminal unit by the side of 60 and a user (It is hereafter described as an agency terminal unit) The terminal unit by the side of 70 and a verification office (It is hereafter described as user-terminal equipment) (It is hereafter described as a verification office terminal unit) It is the network system which consists of an entity (not shown) of a large number containing 30, and each entity is made as [receive / deliver and / digital data / mutually / through a network].

[0083] The server terminal unit 50 is made as [transmit / the output of the primary decode processing section 52 / to user-terminal equipment 70] while having the primary encryption processing section 51 to which image data (digital data) is supplied, and the primary decode processing section 52 to which the data from user-terminal equipment 70 and the verification office terminal unit 30 are supplied and transmitting the output of the primary encryption processing section 51 to the agency terminal unit 60.

[0084] The agency terminal unit 60 is equipped with the contract check processing section 61 to which the data from user-terminal equipment 70 are supplied, and the digital-watermarking embedding processing section 62 to which the output of the primary encryption processing section 51 of the server terminal unit 50 is supplied, and is made as [transmit / the output of the digital-watermarking embedding processing section 62 / to user-terminal equipment 70 and the verification office terminal unit 30].

[0085] The contract generation processing section 71 to which user-terminal equipment 70 transmits data to the contract check processing section 61 of the agency terminal unit 60, The signature generation processing section 72 and the digital-watermarking embedding processing section 73 to which the data from the signature generation processing section 72 and the digital-watermarking embedding processing section 62 of the agency terminal unit 60 are supplied, The secondary encryption processing section 74 to which the output of the digital-watermarking embedding processing section 73 is supplied, It has the secondary decode processing section 75 to which the data from the primary decode processing section 52 of the server terminal unit 50 are supplied, and is made as [output / as image data with digital watermarking / the output of the secondary decode processing section 75]. Moreover, the output of the secondary encryption processing section 74 is made as [supply / respectively / the primary decode processing section 52 of the server terminal unit 50 and the verification office terminal unit 30].

[0086] The verification office terminal unit 30 is equipped with the secondary decode processing section 31 to which the output of the digital-watermarking embedding processing section 62 of the agency terminal unit 60 and the secondary encryption processing section 74 of user-terminal equipment 70 is supplied, and the digital-watermarking check processing section 32 to which the output of the secondary decode processing section 31 is supplied, and is made as [supply / the output of the digital-watermarking check processing section 32 / to the primary decode processing section 52 of the server terminal unit 50].

[0087] Below, operation of the system 300 constituted as mentioned above is explained. In addition, in the protocol shown in this drawing 3 , the information about primary codes, such as a method and a private key, is information which only a server or an author knows, and the information about a secondary code is information which only a user knows. However, among these codes, it shall have the property in which the code will be solved if decode is performed whichever it performs encryption previously. Although explained for hierarchy system like drawing 17 below, if an author is read as a server below, it will become the explanation to the system of drawing 16 .

[0088] [embedding processing] 1 -- first, in user-terminal equipment 70, a user attaches a signature and demands desired image data of the agency terminal unit 60 This demand data is the information (a user's signature information) generated by the contract generation processing section 71, and, below, calls this contract information. In an agency, in the contract check processing section 61, the received contract information is checked from a signature of a user, and image data is required of the server terminal unit 50 (author) after the check. In response, the primary encryption processing section 51 in the server terminal unit 50 performs primary encryption processing E1 () to image data G, and sends the obtained data E1 (G) to the agency terminal unit 60.

[0089] 2) Next, in the agency terminal unit 60, the contract check processing section 61 creates the user information U from the contract information received from user-terminal equipment 70. And the digital-watermarking embedding processing section 62 is embedded at the primary encryption image data E1 (G) to which the user information U created in the above-mentioned contract check processing section 61 was sent from the server terminal unit 50, and is sent to user-terminal equipment 70. Therefore, the information on primary encryption image data E1(G)+U with user information will be sent to user-terminal equipment 70.

[0090] At this time, the digital-watermarking embedding processing section 62 of the agency terminal unit 60 sends the confidential information about digital watermarking to the verification office terminal unit 30. In addition, confidential information is information about the embedding position and intensity for detecting digital watermarking, and it is enciphered and sent by other cipher systems currently shared with the verification office terminal unit 30.
[0091] 3) Next, in user-terminal equipment 70, the signature generation processing section 72 generates the signature information S using its own private key. And the digital-watermarking embedding processing section 73 embeds the signature information S generated in the signature generation processing section 72 at primary (distributed) encryption image data E1(G)+U sent from the agency terminal unit 60. Moreover, the secondary encryption processing section 74 enciphers secondary primary encryption image data E1(G)+U+S where the signature information S was embedded in the digital-watermarking embedding processing section 73, and sends it to the verification office terminal unit 30. Therefore, the information on the secondary encryption image data E2 (E1(G)+U+S) will be sent to the verification office terminal unit 30.
[0092] At this time, the secondary encryption processing section 74 of user-terminal equipment 70 generates and signs the hash value H2 to the transmit data (secondary encryption image data E2 (E1(G)+U+S)) to the verification office terminal unit 30, and sends both the confidential information relevant to digital watermarking, and the private key of secondary encryption to the verification office terminal unit 30.
[0093] 4) Next, in the verification office terminal unit 30, check being [of the hash value H2 sent from user-terminal equipment 70] a signature, and that the hash value H2 is in agreement with the hash value of transmit data, and after the check, the secondary decode processing section 31 decodes the secondary encryption image data E2 (E1(G)+U+S) from user-terminal equipment 70, and extracts the user information U and the signature information S from there. And the above-mentioned user information U and the signature information S are inspected in the digital-watermarking check processing section 32, if right, verification information will be created and the signature of the verification office terminal unit 30 will be attached. Finally, the verification office terminal unit 30 sends the secondary encryption image data E2 (E1(G)+U+S) and hash value H2 which were transmitted from user-terminal equipment 70, its signature and the verification information over it, and its signature to the server terminal unit 50.
[0094] 5) Next, in the server terminal unit 50, an author checks the verification information sent from the verification office terminal unit 30, and its signature, and checks the secondary [further] encryption image data E2 (E1(G)+U+S), a hash value H2, and its signature. After the check, the primary decode processing section 52 decodes primary encryption of the above-mentioned secondary encryption image data E2 (E1(G)+U+S), generates the information on E2(G)+D1 (E2 (U+S)), and sends it to user-terminal equipment 70.
[0095] 6) Next, in user-terminal equipment 70, the secondary decode processing section 75 decodes secondary encryption of the information on E2(G)+D1 (E2 (U+S)) sent from the server terminal unit 50, and takes out the image data Gw with digital watermarking. Therefore, the image data Gw with digital watermarking is expressed as Gw=G+D1 (U+S). This shows that the user information U and a user's signature information S that it was influenced of primary decode to image data G of a basis space, and it is embedded as information.
[0096] When the right watermark information is not verified with the verification office terminal unit 30 in the process of the above 4 according to one of the injustice of an author or a user, the server terminal unit 50, the agency terminal unit 60, and user-terminal equipment 70 are told about that. Even if dealings are stopped at this time, neither profits nor disadvantageous profit is for anyone, and there is no meaning which carries out injustice. In addition, when illegal copy (unjust picture) Gw' is discovered, an inaccurate person can be easily specified by the easy following verification processings. However, here above-mentioned reference [1] [2] Image data sets similarly assumption of not receiving deformation and elimination of watermark information.
[0097] [verification processing] 1 -- first, in the server terminal unit 50, an author enciphers primary discovered unjust picture Gw', and extracts user information When user information is not extracted here, it presumes that an author is inaccurate.
2) On the other hand, when the right user information is extracted, extract signature information from the data which enciphered the primary above-mentioned unjust picture Gw'.
3) Here, when the right signature information is extracted, presume that a user is inaccurate. Being able to create [but] only to a user the signature information that this is right, an author and an agency are because signature information cannot be known.
4) Moreover, when the right signature information is not extracted, presume that an author is inaccurate.
[0098] By the digital-watermarking method by this 3rd operation form, since encryption processing of digital data and embedding processing of digital-watermarking information are performed by three persons of the server terminal unit 50, the agency terminal unit 60, and user-terminal equipment 70 and the verification office terminal unit 30 is checking justification of cipher processing and the embedded digital-watermarking information, even if an author, an agency, or a user copies illegally independently, the malfeasance can be checked easily, and an inaccurate person can also verify easily. Moreover, by this method, since the interest of an author, an agency, and a user conflicts, there cannot be no conspiracy. Even if it conspires, a malfeasance can be checked easily. In addition, the safety of this processing puts a basis on a verification office being reliable.
[0099] [4th operation form] Also in the 4th operation form, the processing by which the server or author who showed drawing 16 or drawing 17 hands a user digital data through an agency is collectively considered like the 3rd operation form. Hereafter, the 4th operation form concerning this invention is explained, referring to drawing 4 . That is, the digital-watermarking method concerning the 4th operation form is carried out by the system 400 as shown in drawing 4 , and this system 400 is also

what applied the electronic-intelligence distribution system concerning this invention.
[0100] The system 400 concerning the 4th operation form is a network system which consists of an entity (not shown) of a large number containing the server terminal unit 50, the agency terminal unit 60, user-terminal equipment 70, and the verification office terminal unit 30, and each entity is made as [receive / deliver and / digital data / mutually / through a network].
[0101] The server terminal unit 50 is made as [transmit / the output of the primary decode processing section 52 / to user-terminal equipment 70] while having the primary encryption processing section 51 to which image data (digital data) is supplied, and the primary decode processing section 52 to which the data from the agency terminal unit 60 and the verification office terminal unit 30 are supplied and transmitting the output of the primary encryption processing section 51 to the agency terminal unit 60.
[0102] The contract check processing section 61 to which, as for the agency terminal unit 60, the data from user-terminal equipment 70 are supplied, The digital-watermarking embedding processing section 62 to which the output of the contract check processing section 61 and the primary encryption processing section 51 of the server terminal unit 50 is supplied, While having the digital-watermarking embedding processing section 63 to which the data from user-terminal equipment 70 are supplied and transmitting the output of one digital-watermarking embedding processing section 62 to user-terminal equipment 70 It is made as [transmit / the output of the digital-watermarking embedding processing section 63 of another side / to the server terminal unit 50 and the verification office terminal unit 30].
[0103] The contract generation processing section 71 to which user-terminal equipment 70 transmits data to the contract check processing section 61 of the agency terminal unit 60, The signature generation processing section 72 and the secondary encryption processing section 74 to which the output of the digital-watermarking embedding processing section 62 of the agency terminal unit 60 is supplied, It has the secondary decode processing section 75 to which the data from the primary decode processing section 52 of the server terminal unit 50 are supplied, and is made as [output / as image data with digital watermarking / the output of the secondary decode processing section 75]. Moreover, the output of the secondary encryption processing section 74 is made as [supply / respectively / the digital-watermarking embedding processing section 63 of the agency terminal unit 60 and the verification office terminal unit 30].
[0104] The secondary decode processing section 31 to which, as for the verification office terminal unit 30, the output of the digital-watermarking embedding processing section 63 of the agency terminal unit 60 and the secondary encryption processing section 74 of user-terminal equipment 70 is supplied, It has the digital-watermarking check processing section 32 to which the output of the secondary decode processing section 31 and the digital-watermarking embedding processing section 63 of the agency terminal unit 60 is supplied, and is made as [supply / the output of the digital-watermarking check processing section 32 / to the primary decode processing section 52 of the server terminal unit 50].
[0105] Below, operation of the system 400 constituted as mentioned above is explained. In addition, in the protocol shown in this drawing 4 , the information about primary codes, such as a method and a private key, is information which only a server or an author knows, and the information about a secondary code is information which only a user knows. However, among these codes, it shall have the property in which the code will be solved if decode is performed whichever it performs encryption previously. Although explained for hierarchy system like drawing 17 below, if an author is read as a server below, it will become the explanation to the system of drawing 16 .
[0106] [embedding processing] 1 -- first, in user-terminal equipment 70, a user attaches a signature and demands desired image data of the agency terminal unit 60 This demand data is the information (a user's signature information) generated by the contract generation processing section 71, and, below, calls this contract information. In an agency, in the contract check processing section 61, the received contract information is checked from a signature of a user, and image data is required of the server terminal unit 50 (author) after the check. In response, the primary encryption processing section 51 in the server terminal unit 50 performs primary encryption processing E1 () to image data G, and sends the obtained data E1 (G) to the agency terminal unit 60.
[0107] 2) Next, in the agency terminal unit 60, the contract check processing section 61 creates the user information U from the contract information received from user-terminal equipment 70. And the digital-watermarking embedding processing section 62 is embedded at the primary encryption image data E1 (G) to which the user information U created in the above-mentioned contract check processing section 61 was sent from the server terminal unit 50, and is sent to user-terminal equipment 70. Therefore, the information on primary encryption image data E1(G)+U with user information will be sent to user-terminal equipment 70.
[0108] 3) Next, in user-terminal equipment 70, the secondary encryption processing section 74 enciphers secondary primary encryption image data E1(G)+U sent from the agency terminal unit 60, and sends the information on the obtained image data E2 (E1 (G) +U) to the agency terminal unit 60. At this time, in the signature generation processing section 72, a user generates the signature information S which can be created only for itself, and sends to the agency terminal unit 60 with the secondary encryption image data E2 (E1 (G) +U). Moreover, the secondary encryption processing section 74 sends the private key of secondary encryption to the verification office terminal unit 30.
[0109] 4) Next, in the agency terminal unit 60, the digital-watermarking embedding processing section 63 embeds the signature information S similarly sent from user-terminal equipment 70 to the secondary encryption image data E2 (E1 (G) +U) sent from user-terminal equipment 70, and sends it to the verification office terminal unit 30. Therefore, the information on secondary encryption image data E2(E1 (G) +U)+S with signature information will be sent to the verification office terminal unit 30.

[0110] At this time, with the agency terminal unit 60, it generates and signs and the hash value H2 to the transmit data (secondary encryption image data E2(E1 (G) +U) +S) to the verification office terminal unit 30 is sent to the verification office terminal unit 30 with the confidential information relevant to digital watermarking. In addition, confidential information is information about the embedding position and intensity for detecting digital watermarking, and it is enciphered and sent by other cipher systems currently shared with the verification office terminal unit 30.
[0111] 5) Next, the signature of the hash value H2 sent from the agency terminal unit 60 in the verification office terminal unit 30, It checks that the hash value H2 is in agreement with the hash value of transmit data. While extracting the secondary encryption image data E2(E1 (G) +U)+ left-hand-lay signature information S from the agency terminal unit 60 in the digital-watermarking check processing section 32 after the check Secondary encryption of the above-mentioned secondary encryption image data E2(E1 (G) +U)+S is decoded in the secondary decode processing section 31, and the user information U is extracted from there.
[0112] And the digital-watermarking check processing section 32 inspects the user information U and the signature information S which carried out [above-mentioned] extraction, if right, will create verification information and will attach the signature of the verification office terminal unit 30. Finally, the verification office terminal unit 30 sends secondary encryption image data E2(E1 (G) +U)+S and the hash value H2 which were transmitted from the agency terminal unit 60, its signature and the verification information over it, and its signature to the server terminal unit 50.
[0113] 6) Next, in the server terminal unit 50, an author checks the verification information sent from the verification office terminal unit 30, and its signature, and checks secondary [further] encryption image data E2(E1 (G) +U)+S, a hash value H2, and its signature. After the check, the primary decode processing section 52 decodes primary encryption of the above-mentioned secondary encryption image data E2(E1 (G) +U)+S, generates the information on E2(G)+D1 (E2 (U) +S), and sends it to user-terminal equipment 70.
[0114] 7) Next, in user-terminal equipment 70, the secondary decode processing section 75 decodes secondary encryption of the information on E2(G)+D1 (E2 (U) +S) sent from the server terminal unit 50, and takes out the image data Gw with digital watermarking. Therefore, the image data Gw with digital watermarking is expressed as Gw=G+D1 (U+D2 (S)). This shows that the user information U influenced of primary decode to image data G of a basis and the signature information S influenced of secondary [further] decode space, and it is embedded as information.
[0115] When the right watermark information is not verified with the verification office terminal unit 30 in the process of the above 5 according to one of the injustice of an author or a user, the server terminal unit 50, the agency terminal unit 60, and user-terminal equipment 70 are told about that. Even if dealings are stopped at this time, neither profits nor disadvantageous profit is for anyone, and there is no meaning which carries out injustice. In addition, when illegal copy (unjust picture) Gw' is discovered, an inaccurate person can be easily specified by the easy following verification processings. However, here above-mentioned reference [1] [2] Image data sets similarly assumption of not receiving deformation and elimination of watermark information.
[0116] [verification processing] 1 -- first, in the server terminal unit 50, an author enciphers primary discovered unjust picture Gw', and extracts user information U' When user information U' is not extracted here, it presumes that an author is inaccurate. 2) on the other hand -- being right -- a user -- information -- extracting -- having had -- a case -- a server -- a terminal unit -- 50 -- one -- order -- enciphering -- having had -- image data -- Gw -- ' -- a user -- information -- U -- ' -- the verification office terminal unit 30 -- being shown -- inspection -- requiring . The verification office terminal unit 30 enciphers secondary image data Gw' by which the primary code was carried out (this encryption function is un-illustrating), and extracts signature information.
3) Here, when the right signature information is extracted, presume that a user is inaccurate.
4) Moreover, when the right signature information is not extracted, presume that an author is inaccurate.
[0117] Since encryption processing of digital data and embedding processing of digital-watermarking information are performed by three persons of the server terminal unit 50, the agency terminal unit 60, and user-terminal equipment 70 and the verification office terminal unit 30 is checking justification of cipher processing and the embedded digital-watermarking information also by the digital-watermarking method by this 4th operation form, even if an author, an agency, or a user copies illegally independently, the malfeasance can be checked easily, and an inaccurate person can also verify easily. Moreover, by this method, since the interest of an author, an agency, and a user conflicts, there cannot be no conspiracy. Even if it conspires, a malfeasance can be checked easily. In addition, the safety of this processing puts a basis on a verification office being reliable.
[0118] [5th operation form] At the time of the purchase of digital data, a user's anonymity is realized like the 2nd operation form, and the 5th operation form enables it to specify an unjust distribution person in the 3rd operation form shown in drawing 3 , when injustice like unjust distribution of a picture is discovered. This is realized by the system 500 as shown in drawing 5 . Although this system 500 is considered as the same composition as the system 300 in the 3rd operation form mentioned above, it is considered as the composition with which the anonymity public key certificate from a certificate authority 40 is given to user-terminal equipment 70.
[0119] When a certificate authority 40 holds correspondence with a public key and its owner secretly with this operation form as well as the 2nd operation form, it is preventing from describing an owner's name in the certificate of a public key. Then, if a user sends the anonymity public key with a certificate for inspecting the signature of contract information, and the signature information S together with contract information in the procedure of one under embedding processing in the 3rd operation form mentioned above, a user can make himself anonymity at the time of the purchase of digital data.

[0120] Therefore, although an anonymity public key with a certificate is passed to an agency as information which specifies a user, at the time of discovery of an illegal copy, a user can be specified by showing the anonymity public key with a certificate in a certificate authority 40, and having a user corresponding to the public key taught. Both the anonymity at the time of a user's digital data purchase and the inaccurate person specification at the time of unjust discovery are realizable by changing as follows the procedure of one under embedding processing stated with the 3rd operation form mentioned above from the above thing, and the procedure of one under verification processing.
[0121] In addition, both the anonymity at the time of a user's digital data purchase and the inaccurate person specification at the time of unjust discovery are realizable also by changing as follows the procedure of one under embedding processing stated with the 4th operation form which prepared and mentioned the certificate authority 40 above to the user-terminal equipment 70 in the system 400 of drawing 4 which shows the 4th operation form, and the procedure of one under verification processing.
[0122] Hereafter, the embedding processing in the system 500 of above-mentioned drawing 5 and verification processing are explained concretely.
[0123] [embedding processing] 1 -- first, in user-terminal equipment 70, together with the anonymity public key with a certificate published by the certificate authority 40, the contract generation processing section 71 attaches the signature corresponding to the public key for the contract information which requires desired image data, and sends it to the agency terminal unit 60 In an agency, in the contract check processing section 61, the received contract information is checked from an anonymity public key, and image data is required of an author after the check. In response, the primary encryption processing section 51 in the server terminal unit 50 performs primary encryption processing E1 () to image data G, and sends the obtained data E1 (G) to the agency terminal unit 60. Since the following procedures of 2-6 are the same as the procedure stated with the 3rd operation form, the explanation which overlaps here is omitted.
[0124] In the [verification processing] 1 server terminal unit 50, primary code each processing section 51 enciphers primary discovered unjust picture Gw', and extracts user information. And the anonymity public key which the extracted user information and contract information show is shown in a certificate authority 40, and the user name corresponding to the anonymity public key is heard. When user information is not extracted here, it presumes that an author is inaccurate. The following procedures of 2-4 are the same as the procedure stated with the 3rd operation form.
[0125] As stated above, according to the 5th operation form, anonymity can maintain a user also to a verification office at the time of the purchase of digital data.
[0126] above-mentioned the 1- the various data containing the image data shown in the 5th operation form and the hash value obtained by embedding processing of digital-watermarking information are storable by the following picture formats For example, in the following general picture format, the image data sent in each stage can be stored in the image data section, and the hash value corresponding to it, its signature, etc. can be stored in a picture header unit. Moreover, the hash value which a user finally needs to save and its signature, the key of a secondary code, etc. can be stored in a picture header unit, and image data with digital watermarking can be stored in the image data section.
[0127] On the other hand, in the FlashPixTM file format shown below, the general picture format including the above hash value or its signature is storable as data of each hierarchy. Moreover, a hash value, its signature, etc. are also storable in a property set as attribute information.
[0128] First, a general picture format is explained. In a general picture format, as shown in drawing 6 , an image file is divided into a picture header unit and the image data section.
[0129] Generally, when reading image data in the image file, required information and the supplementary information explaining the contents of a picture are stored in a picture header unit. In the example of drawing 6 , information, such as offset to the picture format identifier which shows the picture format name, a file size, the width of face, the height and the depth of a picture, compressive existence, resolution, and the storing position of image data, and size of a color palette, is stored. On the other hand, the image data section is a portion which stores image data one by one. As a typical example of such a picture format, it is Microsoft. The BMP format of a shrine, the GIF format of Compuserve, etc. have spread widely.
[0130] Next, a FlashPixTM file format is explained concretely. In the FlashPixTM (FlashPix is registered trademark of U.S. Eastman Kodak) file format explained henceforth, the image data stored in the picture attribute information and the image data section which were stored in the above-mentioned picture header unit is structured further, and is stored in a file. This structured image file is shown in drawing 7 and drawing 8 . Each property and data in a file are accessed by the storage and the stream equivalent to the directory of MS-DOS, and a file. In above-mentioned drawing 7 and drawing 8 , a portion with a shadow is storage and a shadow-less portion is a stream. Image data and picture attribute information are stored in a stream portion.
[0131] In drawing 7 , image data is hierarchized in different resolution, calls the picture of each resolution Subimage, and has shown it by Resolution 0 and 1, --, n. Information required in order to read the image data is Subimage Header to the picture of each resolution. Image data is Subimage data again. It is stored. A property set classifies and defines attribute information according to the purpose of use and contents, and is Summary info.Property Set, Image info.Property Set, Image Content Property Set, and Extention list property Set. It is.
[0132] [Explanation of each property set] Summary info.Property Set is not peculiar to FlashPix, and is Microsoft. In the SUTORAKU Chard storage of a shrine, it is an indispensable property set and the title, the title, author, thumbnail picture, etc. of the file are stored. Moreover, the general information about the storage section (Strage) is stored in Comp Obj.Stream.
[0133] Image Content Property Set is an attribute which describes the storing method of image data (refer to drawing 9). For

this attribute, the definition of the quantization table Huffman table at the time of using the composition of the number of hierarchies of image data, the width of face and the height of the picture of the degree of maximal-solution image, the width of face about the picture of each resolution, height, and a color or JPEG compression etc. is described. Extention list property Set It is the field used in case the information which is not included in the basic specification of Above FlashPix is added. Furthermore, ICC Profile The conversion profile for the color space conversion specified in ICC (International Color Consortium) is described by the portion.

[0134] Moreover, various information which can be used in case image data is used, for example, the picture, is incorporated how, and Image info.Property Set stores the following information on the ability to use [how].

- the contents (the person in a picture --) of the information and picture about the information and copyright about how [to incorporate digital data]/or a generation method Setting of the camera at the time of the information and photography about the camera used for the information and photography about a place etc. (exposure) The maker name of the information and film about the resolution peculiar to information and a digital camera and the mosaic filters of shutter speed, a focal distance, and flash plate use, such as existence Information about the scanner which was used in the case of the information and the scanning picture about a kind and size in case information and original, such as a product name and a kind (a negative/positive, a color/black and white), are a book and printed matter, or software and the person who operated it [0135] FlashPix Image View Object of drawing 8 is an image file which doubles and stores the viewing parameter and image data which are used in case a picture is displayed. A viewing parameter is the set of the processing coefficient which memorizes processing of rotation of a picture, expansion/reduction, movement, color conversion, and filtering since it is adapted in the case of image display. It sets to this drawing 8 and is Global info.Property Set. The property list locked is described by the portion, for example, the index of the maximum picture, the index of the maximum change item, the last correction person's information, etc. are described.

[0136] Moreover, it sets to this drawing and is Source/Result FlashPix Image Object. It is the substance of FlashPix image data, and Source FlashPix Image Object is indispensable and Result FlashPix Image Object is an option. The image data of the result to which Result FlashPix Image Object carried out the image processing of the image data with original Source FlashPix Image Object using the viewing parameter is stored, respectively.

[0137] Moreover, Source/Result desc.Property Set is a property set for discernment of the above-mentioned image data, and stores the time of Picture ID, the property set of the ban on change, and the last refix date etc. Transform Property Set stores the Affine transform coefficient for rotation of a picture, expansion/reduction, and movement, the color conversion matrix, the contrast adjustment value, and the filtering coefficient.

[0138] Next, the handling of image data is explained. Here, the picture format including the picture of two or more resolution divided into two or more tiles is mentioned as an example, and is explained. The example of the image file which consists of two or more pictures from which resolution differs in drawing 10 is shown. In this drawing 10 , as for the picture of the degree of maximal-solution image, the train x line consists of X0xY0, and it is reduced until the pictures with large resolution are X0/2xY0/2, it reduces a train and a line every [2 / 1/] one by one after it and it comes / each other / 64 pixel or less or] to spread a train and a line on the degree.

[0139] Thus, as a result of hierarchizing image data, the header information and the image data which were explained by the term of a general picture format are needed to "the number of hierarchies in one image file", and the picture of each hierarchy as attribute information on a picture (refer to drawing 6). The information about the width of face of the number of the hierarchies in one image file or the picture of the degree of maximal-solution image, height or the width of face of the picture of each resolution, height, color composition, a compression method, etc. is described in above-mentioned ImageContent Property Set (refer to drawing 9).

[0140] Furthermore, the picture of the layer of each resolution is divided for every tile which becomes by 64 pixel x64 pixel as shown in drawing 11 . If it divides into a 64 pixel x64 pixel tile one by one from the upper left section of a picture, depending on a picture, a null may arise to some tiles of a right end and a soffit. In this case, it is repeating and inserting a low-order-end picture or the lowest edge picture, respectively, and 64 pixel x64 pixel is built.

[0141] In FlashPixTM, the image data in each tile is stored by JPEG compression, a single color, and one of incompressible methods. JPEG compression is ISO/IEC JTC1/SC29. It is the picture compression method by which international standardization was carried out, and explanation of the method itself is omitted here. Moreover, a single color is a method which expresses the color of the tile by one color, without the whole of the one above-mentioned tile recording the value of each pixel, only when [same] **** composition is carried out. Especially this method is effective by the picture generated by CG.

[0142] Thus, the image data by which tile division was carried out is Subimage data of drawing 7 . It is stored in a stream and all of the total of a tile, the size of each tile, the starting position of data, and the compression method are Subimage Header. It is stored (refer to drawing 12).

[0143] [other operation gestalten] -- the 1- described above -- the embedding of watermark information in the 5th operation gestalt, although it is realizable with various technique For example, the reference in "spring water, Numao, and Morimoto (IBM Japan): "static-image data hiding by pixel block", the 53rd time national conference of Information Processing Society of Japan, and 1N-11 month, and September, Heisei 8", "I. J.Cox and J.Kilian, T. Leighton and T.shamoon (NEC) :"Sucure Spread Spectrum Watermarking for Multimedia" NECReserch Institure It is realizable with the well-known technique to embed as shown in the reference of Technical Report 95-10."

[0144] Moreover, although the cipher system used as a primary code and a secondary code is also realizable with various

methods, it is realizable with the cipher system of changing arrangement of a bit according to a cryptographic key, for example. Moreover, a hash value and its signature can also be attached and sent to all transmit data. Furthermore, although a primary code and a secondary code are used in order not to tell mutual information in embedding processing of watermark information, in order to prevent tapping and the alteration on the channel from a third person, codes, Hash Functions, etc., such as DES (Data Encryption Standard), may be independently used for them.

[0145] moreover, above-mentioned the 1- in the 5th operation gestalt, although the 1st entity (a server or author) is performing detection of unjust distribution, if it has even the extraction means of digital watermarking even if it does not know the private key about a primary code or a secondary code, the user information on unjust distribution and unjust distribution can be known to anyone Then, since what is necessary is to tell a 1st entity side about unjust distribution discovery, and just to start verification processing, the discoverer of unjust distribution is not limited to the 1st entity.

[0146] Moreover, the 1st entity or agency can also embed other information, such as copyright information and information about the distribution situation of the image data, at image data not only the user information U but if needed. Moreover, if embedding processing is performed after primary encryption to embed secret information by the 1st entity, signature information and the information similarly influenced of the primary code can be embedded. Furthermore, the user information U does not always need to be before primary encryption, and you may also embed it after primary encryption (only those who know the private key of the 1st entity or a primary code can perform detection of the user information U in this case).

[0147] Moreover, when it is a user using the 2nd printer, terminal, etc. with a common entity, the 2nd signature information and secondary code of an entity may contain the signature information and cipher system of a printer or a common terminal. Moreover, even if primary encryption information from the 1st entity does not have the request using the contract information from the 2nd entity, it may be widely distributed by the network, CD-ROM, etc. Moreover, the information (information like a personal identification number) which it did not need to be generated by the public key cryptosystem and the user defined for contract information etc. is sufficient as the signature information S on the 2nd entity.

[0148] Moreover, in the U.S., when using a code 40 bits or more, in order to prevent improper use of a code, the key Administration Bureau which manages a cryptographic key is needed. Then, it is also possible to make a verification office serve as the key Administration Bureau. Therefore, if a verification office also performs the surveillance of an unjust picture when the verification office has managed the key of a secondary code beforehand, a verification office can perform above-mentioned verification processings 1-3 independently. The key of the primary code of the 1st entity may be ****(ed) by the same verification office, and may be managed by other key Administration Bureau. Moreover, the key Administration Bureau may generate and distribute the key of the 1st entity or the 2nd entity.

[0149] Moreover, an agency does not restrict that it is one but may be constituted hierarchical. At this time, the agency in charge [in a hierarchy] may represent the processing which an agency performs, it may be performed, the above-mentioned protocol is performed among agencies, and it may be made to clarify responsibility. Moreover, when the number of agencies is one like drawing 17 , the embedding of the user information U1 about an agency can be omitted.

[0150] Moreover, although he is to send the primary coding information E1 of image data G (G) to an agency after an author is required, you may make him send beforehand the primary encryption image data E1 (G) to an agency. Moreover, although the agency after the 3rd operation gestalt does not have code E3() and decode D3 (), after data are sent to the beginning from an author, before enciphering by code E3 () and sending data to an author finally, you may decode by decode D3 ().

[0151]

[Effect of the Invention] According to the digital-watermarking method and electronic-intelligence distribution system of this invention, so that clearly from above-mentioned explanation Distribute by two or more meanses or entities, and cipher processing and digital-watermarking embedding processing to data are performed. Since one [at least] justification of the above-mentioned cipher processing performed by the means or entity of the above-mentioned plurality and digital-watermarking embedding processing was verified by the means, the means different from an entity, or entity of the above-mentioned plurality When distributing by copying data unjustly in the network constituted hierarchical, the malfeasance and a malfeasance person can be recognized certainly. By this, it becomes possible to prevent injustice certainly and a safe system can be realized about unjust distribution of data. Furthermore, the application to the key Administration Bureau which prevents a user's anonymity and improper use of a code by this system is also easily realizable.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any
damages caused by the use of this translation.

1. This document has been translated by computer.So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The digital-watermarking method characterized by verifying one [at least] justification of the above-mentioned cipher processing which distributed by two or more meanses or entities, performed cipher processing and digital-watermarking embedding processing to data, and was performed by the means or entity of the above-mentioned plurality, and digital-watermarking embedding processing by the means, the means different from an entity, or entity of the above-mentioned plurality.
[Claim 2] The means or entity of the above-mentioned plurality is a digital-watermarking method according to claim 1 characterized by being at least three or more sorts of meanses or entities.
[Claim 3] The means or the entity of the above-mentioned plurality is a digital-watermarking method according to claim 2 characterized by to consist of the 1st entity which has a means to perform the 1st cipher processing to data, the 2nd entity which has a means to perform the above-mentioned digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above, and the 3rd entity which has a means perform the 2nd cipher processing and uses data with digital watermarking.
[Claim 4] The digital-watermarking method according to claim 2 characterized by providing the following. The means or entity of the above-mentioned plurality is the 1st entity which has a means to perform the 1st cipher processing to data. The 2nd entity which has a means to perform the above-mentioned digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above. The 3rd entity which has a means to perform a means to perform the above-mentioned digital-watermarking embedding processing, and 2nd cipher processing, and uses data with digital watermarking.
[Claim 5] The digital-watermarking method according to claim 2 characterized by providing the following. The means or entity of the above-mentioned plurality is the 1st entity which has a means to perform a means to perform the above-mentioned digital-watermarking embedding processing to data, and 1st cipher processing. The 2nd entity which has a means to perform the above-mentioned digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above. The 3rd entity which has a means to perform the 2nd cipher processing and uses data with digital watermarking.
[Claim 6] The digital-watermarking method according to claim 2 characterized by providing the following. The means or entity of the above-mentioned plurality is the 1st entity which has a means to perform a means to perform the above-mentioned digital-watermarking embedding processing to data, and 1st cipher processing. The 2nd entity which has at least one of the meanses which performs a means to perform the above-mentioned digital-watermarking embedding processing, a means to perform the 1st cipher processing, and 2nd cipher processing, and manages and distributes the data from the 1st entity of the above. The 3rd entity which has a means to perform a means to perform the above-mentioned digital-watermarking embedding processing, and 2nd cipher processing, and uses data with digital watermarking.
[Claim 7] The above-mentioned entity is a digital-watermarking method given in any 1 term of the claims 1-6 characterized by enciphering to the data with which digital watermarking was embedded.
[Claim 8] The above-mentioned entity is a digital-watermarking method given in any 1 term of the claims 1-6 characterized by embedding digital watermarking to the data with which encryption was given.
[Claim 9] The 2nd entity of the above is a digital-watermarking method given in any 1 term of the claims 3-6 characterized by embedding digital watermarking to the data with which the 1st cipher processing of the above from the 1st entity of the above was performed.
[Claim 10] The 2nd entity of the above is a digital-watermarking method according to claim 3 characterized by embedding digital watermarking to the data with which the 2nd cipher processing of the above from the data with which the 1st cipher processing of the above from the 1st entity of the above was performed, and the 3rd entity of the above was performed.
[Claim 11] The 2nd entity of the above is a digital-watermarking method according to claim 10 characterized by outputting the value which, on the other hand, changed the data with which the 2nd cipher processing of the above was performed with the tropism function.
[Claim 12] The 2nd entity of the above is a digital-watermarking method according to claim 11 characterized by transmitting the value changed with the above-mentioned 1 directivity function to the 4th entity of the above.
[Claim 13] The 3rd entity of the above is a digital-watermarking method given in any 1 term of the claims 3-6 characterized by outputting with the data with which the value which, on the other hand, changed the data with which the 2nd cipher

processing of the above was performed with the tropism function was given to the 2nd cipher processing of the above.
[Claim 14] The 3rd entity of the above is a digital-watermarking method according to claim 13 characterized by transmitting the value changed with the above-mentioned 1 directivity function to the 4th entity of the above.
[Claim 15] The 3rd entity of the above is a digital-watermarking method given in any 1 term of the claims 3-6 characterized by receiving the information enciphered primarily beforehand and giving secondary encryption to the this enciphered information.
[Claim 16] The 4th entity of the above is a digital-watermarking method given in any 1 term of the claims 3-6 characterized by it being possible to perform decode processing corresponding to the 2nd cipher processing of the above.
[Claim 17] The 4th entity of the above is a digital-watermarking method given in any 1 term of the claims 3-6 characterized by having a means to manage a cryptographic key.
[Claim 18] The 4th entity of the above is a digital-watermarking method according to claim 17 characterized by verifying one [at least] justification of the above-mentioned digital watermarking and cipher processing by decrypting the data which are outputted from other entities and with which it was enciphered and digital watermarking was embedded.
[Claim 19] The 4th entity of the above is a digital-watermarking method according to claim 17 or 18 characterized by verifying one [at least] justification of the above-mentioned digital watermarking and cipher processing by comparing the value which, on the other hand, changed the data which are outputted from an entity besides the above, and with which it was enciphered and digital watermarking was embedded with the tropism function with the value outputted from an entity besides the above.
[Claim 20] The electronic-intelligence distribution system which transmits and receives digital data on the network system which consists of two or more entities and which is characterized by providing the following. The 1st entity which has a means to perform the 1st cipher processing to data. The 2nd entity which has a means to perform digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above. The 3rd entity which has a means to perform the 2nd cipher processing and uses data with digital watermarking. The 4th entity which verifies one [at least] justification of cipher processing performed by the above 1st - the 3rd entity, and digital-watermarking embedding processing.
[Claim 21] The electronic-intelligence distribution system which transmits and receives digital data on the network system which consists of two or more entities and which is characterized by providing the following. The 1st entity which has a means to perform the 1st cipher processing to data. The 2nd entity which has a means to perform digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above. The 3rd entity which has a means to perform a means to perform the above-mentioned digital-watermarking embedding processing, and 2nd cipher processing, and uses data with digital watermarking. The 4th entity which verifies one [at least] justification of cipher processing performed by the above 1st - the 3rd entity, and digital-watermarking embedding processing.
[Claim 22] The electronic-intelligence distribution system which transmits and receives digital data on the network system which consists of two or more entities and which is characterized by providing the following. The 1st entity which has a means to perform a means to perform digital-watermarking embedding processing to data, and 1st cipher processing. The 2nd entity which has a means to perform the above-mentioned digital-watermarking embedding processing, and manages and distributes the data from the 1st entity of the above. The 3rd entity which has a means to perform the 2nd cipher processing and uses data with digital watermarking. The 4th entity which verifies one [at least] justification of cipher processing performed by the above 1st - the 3rd entity, and digital-watermarking embedding processing.
[Claim 23] The electronic-intelligence distribution system which transmits and receives digital data on the network system which consists of two or more entities and which is characterized by providing the following. The 1st entity which has a means to perform a means to perform digital-watermarking embedding processing to data, and 1st cipher processing. The 2nd entity which has at least one of the meanses which performs a means to perform the above-mentioned digital-watermarking embedding processing, a means to perform the 1st cipher processing, and 2nd cipher processing, and manages and distributes the data from the 1st entity of the above. The 3rd entity which has a means to perform a means to perform the above-mentioned digital-watermarking embedding processing, and 2nd cipher processing, and uses data with digital watermarking. The 4th entity which verifies one [at least] justification of cipher processing performed by the above 1st - the 3rd entity, and digital-watermarking embedding processing.
[Claim 24] The 4th entity which performs the above-mentioned verification is an electronic-intelligence distribution system given in any 1 term of the claims 20-23 characterized by being the entity which manages a cryptographic key.
[Claim 25] The digital-watermarking information which the 1st entity of the above embeds is an electronic-intelligence distribution system according to claim 22 or 23 characterized by including the information about the 3rd entity of the above.
[Claim 26] The digital-watermarking information which the 1st entity of the above embeds is an electronic-intelligence distribution system according to claim 22 or 23 characterized by including the information about the digital data which transmits.
[Claim 27] The digital-watermarking information which the 2nd entity of the above embeds is an electronic-intelligence distribution system given in any 1 term of the claims 20-23 characterized by including the information about the 3rd entity of the above.
[Claim 28] The digital-watermarking information which the 3rd entity of the above embeds is an electronic-intelligence distribution system according to claim 21 or 23 characterized by being the information which can create only the 3rd entity of the above.

[Claim 29] The 1st entity of the above is an electronic-intelligence distribution system according to claim 22 or 23 characterized by performing the above-mentioned digital-watermarking embedding processing after verifying the signature of the 3rd entity of the above with the anonymity public key with a certificate published by the certificate authority.
[Claim 30] The 2nd entity of the above is an electronic-intelligence distribution system given in any 1 term of the claims 20-23 characterized by performing the above-mentioned digital-watermarking embedding processing after verifying the signature of the 3rd entity of the above with the anonymity public key with a certificate published by the certificate authority.

[Translation done.]